Unmanned Ground Vehicles for Integrated Force Protection

Daniel M. Carroll[*a], SMSgt Kenneth Mikell[b], Thomas Denewiler[c]
[a]SSC San Diego, 53560 Hull Street, San Diego, CA 92152
[b]United States Air Force (USAF) Force Protection Battlelab (FPB),1517 Billy Mitchell Blvd, Bldg 954, Lackland AFB, TX 78236-0119
[c]Science Applications International Corporation (SAIC), 3990 Old Town Avenue, Suite 304C, San Diego, CA 92110

ABSTRACT

The combination of Command and Control (C2) systems with Unmanned Ground Vehicles (UGVs) provides Integrated Force Protection from the Robotic Operation Command Center. Autonomous UGVs are directed as Force Projection units. UGV payloads and fixed sensors provide situational awareness while unattended munitions provide a less-than-lethal response capability. Remote resources serve as automated interfaces to legacy physical devices such as manned response vehicles, barrier gates, fence openings, garage doors, and remote power on/off capability for unmanned systems.

The Robotic Operations Command Center executes the Multiple Resource Host Architecture (MRHA) to simultaneously control heterogeneous unmanned systems. The MRHA graphically displays video, map, and status for each resource using wireless digital communications for integrated data, video, and audio. Events are prioritized and the user is prompted with audio alerts and text instructions for alarms and warnings. A control hierarchy of missions and duty rosters support autonomous operations.

This paper provides an overview of the key technology enablers for Integrated Force Protection with details on a force-on-force scenario to test and demonstrate concept of operations using Unmanned Ground Vehicles. Special attention is given to development and applications for the Remote Detection Challenge and Response (REDCAR) initiative for Integrated Base Defense.

Keywords: Force protection, unmanned ground vehicle, command and control, integrated base defense

1. INTRODUCTION

The Robotic Operations Command Center (ROCC) is a tactical operations center for deploying and monitoring unmanned systems in and around SSC San Diego's Seaside robotics facility. Testing and evaluation is performed in the ROCC for Command and Control (C2) for Unmanned Ground Vehicles (UGVs). The C2 component for the ROCC is SSC San Diego’s Multiple Resource Host Architecture (MRHA) software. Mobile Detection Assessment Response System (MDARS) patrol units are security UGVs deployed from the ROCC. An application for C2 for UGV is the Integrated Base Defense (IBD) developed by the United States Air Force.

Unmanned Systems, Command and Control (C2), Network-Centric Communications, and Intelligence, Surveillance, and Reconnaissance (ISR) are key enabling technologies demonstrated from the Robotics Operations Command Center (ROCC). Legacy Physical Security Equipment is connected to the C4ISR infrastructure – an example is a swing-arm barrier gate typically installed at checkpoints. A Force-On-Force scenario demonstrates the potential force multiplication factors with C4ISR of unmanned systems for Integrated Force Protection.

Spiral development for MDARS includes interoperability for communications, payloads, and user interfaces. The Air Force Remote Detection Challenge and Response (REDCAR) initiative is a System of Systems approach that includes MDARS and SCOUT, designed by AFRL Robotics Group, to address the unmanned component for IBD.

*Daniel.Carroll@navy.mil; phone 1 619 553-7636; fax 1 619 553-6188; http://www.spawar.navy.mil/robots/

2. BACKGROUND

a. Robotic Operations Command Center (ROCC)

The ROCC control room (Fig. 1) contains a three-bay guard console with 19-inch monitors, three wall-mounted Hitachi 37-inch plasma display panels, ten stadium-style theater seats for visitors, a 5.1 channel Dolby surround sound system, adjustable overhead lighting, and a DirecTV satellite dish for monitoring news and information.

The ROCC command and control console is based upon the SSC San Diego's Multiple Resource Host Architecture (MRHA), a distributed processing system that allows coordinated control of multiple autonomous resources, including up to 255 unmanned vehicles and/or unmanned sensors. The MRHA software components for Supervisor, Video Server, and Operator Station are displayed on the three monitors on the console. The displays are mirrored on the overhead panels for viewing from the seating area.

The ROCC equipment room is located adjacent to the control room and contains a two-console KVM switch that enables operation of the system from either location. The MRHA components are hosted on six rack-mounted Pentium-class computers. An *Extron DVS 150* video scaler converts RGB, S-video, and composite video signals to RGB-HV and SXGA video for viewing on the plasma panels. A *Color Simplex Multiplexer* from ROBOT Corporation allows up to nine (digital or analog) video streams to be displayed simultaneously on the center panel.

Fig. 1. Robotics Operations Command Center (ROCC)

Fig. 2. Mobile Detection Assessment Response System (MDARS)

b. Mobile Detection Assessment Response System (MDARS)

Mobile Detection Assessment Response System (MDARS) deploys robotic patrol units (Fig. 2) equipped with mission payload suites. MDARS is designed to operate in exterior environments, such as materiel storage yards, arsenals, petroleum storage areas, airfields, rail yards, and port facilities. The objective of MDARS is to provide standardized, semi-autonomous Intrusion Detection System (IDS) using unmanned vehicle technology.

The United States Army Office of the Product Manager, Force Protection Security Equipment (PM-FPS), at Fort Belvoir, VA, is the program manager for the MDARS acquisition program. The United States Army Maneuver Support Center (MANSCEN) is the combat developer. SSC San Diego is the technical director and MRHA software developer. General Dynamics Robotic Systems (GDRS) is the systems integrator and prime contractor.

MDARS meets the Army's requirement for a semi-autonomous mobile capability for patrolling physical security sites. With minimal operator intervention other than system initiation, the patrol unit automatically moves randomly to and throughout designated patrol areas in exterior environments primarily during non-duty hours. While on random patrol, the patrol unit will semi-autonomously conduct surveillance, check for intruders, conduct product inventory, and check the status of facility barriers, such as gate and bunker/container doors. Operator input from the control station will be required only if an intruder is detected or the patrol unit encounters an abnormal situation. If the MDARS patrol unit detects an intruder, the video link to the control station is activated and an audio/visual alarm will be annunciated at the control station. This allows security forces the ability to see, hear, and talk/challenge the intruder as well as send the patrol unit to a location where the intruder has been detected. The patrol unit can also read the status of locks on storage structures (open or closed), and can determine the status of inventory items through the use of specialized Radio Frequency (RF) transponder tags.

c. Integrated Base Defense (IBD)

The United States Air Force (USAF) has changed the way it does business in defending its assets and now operates to the concept of Integrated Base Defense (IBD). Approximately two years ago, the Director of USAF Security Forces commissioned a study called Integrated Base Defense (Fig. 3). The premise of the study was that the way the Security Forces defended Air Force assets had essentially remained the same since the Second World War. Although the doctrine was sound, recognizing proven methods like defense in depth and all round defense, it was apparent that the increasing availability of technology impacted upon the current methods employed.

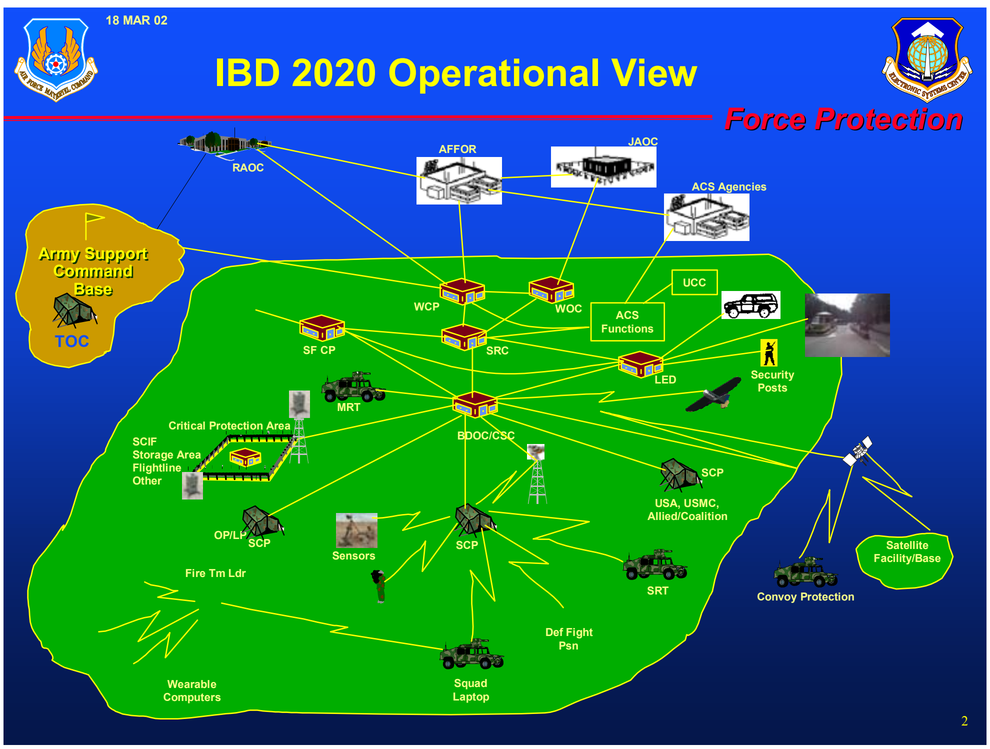

Fig. 3. Integrated Base Defense (from IBD 2020 Technology Architecture)

As the Air Force Security Forces Center developed the IBD objectives and principles, an associated initiative conducted within the Air Force, Force Protection Battlelab (FPB) looked at all aspects of the problem, including tactics, techniques and procedures, equipment and training. FPB highlighted problems of detection, interception and neutralization. Using its Modeling and Simulation Division, FPB developed a Systems Effectiveness Assessment (SEA) model employing force on force programs like the Joint Conflict and Tactical Simulation (JCATS) and Analytic System and Software for Evaluating Safeguards and Security (ASSESS). Rather than look at individual areas of concern, the SEA process looked at the overall current system as a whole. Data was collected that supported the IBD study, with the main findings being that Security Forces had limitations in detecting, intercepting and neutralizing a penetrative threat against an air base or installation. Finding better detection systems and buying time for the defenders to deploy and neutralize the threat became the focus for the FPB.

The Force Protection Battlelab looked at a variety of programs to buy time for the defender and conducted a number of short studies, along with market research, to see if technology could help close the gap. A partial solution was identified that would improve detection, enable some kind of challenge, and allow the Security Forces time to deploy and neutralize the threat. The system of systems incorporated perimeter sensors for detection, cameras for surveillance, and a sound and visual display box that would conduct a challenge. The final part of the system was remotely operated weapons that could be brought to bear on the intruders.

The FPB examined at various fixed configurations and rail/surveillance systems, along with their associated deployment tradeoffs. The challenge system considered using a series of line sensors with associated sound boxes. The initial challenge would be of low intensity, warning the intruders they were entering a restricted area, and to turn back. If the intruders ignored the challenge and continued to move towards Air Force assets, each line sensor they crossed would be associated with an increasing level of challenge from the associated area speakers. Eventually, a final warning would be given before neutralizing action was taken, by either lethal or non-lethal systems. However, this entailed the use of a large number of sound and visual systems. Attaching sensors and response devices on a monorail proved to be much more technically challenging than expected. Film producers and sports coverage systems had neither the range nor speed to meet the requirements.

An alternative approach was considered to use robotics platforms in the force protection role and unmanned ground vehicles were combined with sensor technology into REDCAR (Remote Detection Challenge and Response) using an integrated family of robotics platforms. Deploying REDCAR robotics platforms around an air base or installation would help to delay or mitigate an aggressor's progress, thereby allowing Security Forces to mount an effective and timely counter.

3. INTEGRATED FORCE PROTECTION

a. Technology Enablers

Unmanned Systems, Command and Control (C2), Network-Centric Communications, and Intelligence, Surveillance, and Reconnaissance (ISR) payloads are key enabling technologies for Integrated Force Protection from the Robotics Operations Command Center (ROCC).

Unmanned vehicles are directed as Force Projection units. They can be rapidly deployed and operated in both fixed and contingency operations. The primary force protection unmanned vehicle for the ROCC is the MDARS patrol unit. The MDARS vehicles have autonomous navigation and obstacle avoidance capabilities and operate payloads for intruder detection, barrier assessment, and product assessment. Proof-of-concept payloads for less-than-lethal weapons and marsupial robots were deployed on MDARS prototype patrol units. A COTS paintball gun loaded with pepper ball ammunition was designed to facilitate experimentation with weapon aiming and firing techniques from the MRHA. An Integrated Marsupial Delivery System was developed to transport smaller deployable assets, such as man-portable UGVs and/or unmanned aerial vehicles (UAV).

The C2 graphically displays video, map, and status for each resource. The C2 for the ROCC is the MRHA. A control hierarchy of missions and duty rosters support autonomous operations. The unmanned systems report all exceptional events and activities to the control station where a human operator monitors their actions. Events are prioritized and the user is prompted with audio alerts and text instructions for alarms and warnings. Multiple intruders are displayed on maps with icon identification for friend or foe an individual track histories. Videos from up to 5 separate unmanned systems are simultaneously displayed. The MRHA also monitors the infrastructure support equipment, such as communication relays, and reports failures to the operator.

All resources including manned and unmanned platforms are connected over wireless digital communications for integrated data, video, and audio. For testing and demonstration purposes only, the communications infrastructure is based on commercial 802.11b 2.4GHz radios. The deployed configuration incorporates encryption, military frequency bands, and redundant networks with significant improvements for information assurance and reliable communications. The infrastructure will send encrypted data over the primary channel using high-frequency military radios. A backup, low-frequency radio network (also in a military frequency band) will provide redundancy when the primary network experiences lost communications.

Unmanned payloads and fixed sensors provide situational awareness using Intelligence, Surveillance, and Reconnaissance (ISR) payloads. Unattended munitions provide a less-than-lethal response capability.

The combination of Command and Control (C2) systems with Unmanned Ground Vehicles (UGVs) provides Integrated Force Protection from the Robotic Operation Command Center.

b. Legacy Physical Security Equipment (PSE)

The ROCC supports integration with the legacy Physical Security Equipment (PSE), including remote control of installed equipment such as swing-arm gates (Fig. 4), garage doors, and fence openings using Network-Enabled Resource Devices (NERDs). The installed equipment is activated either autonomously by the MRHA or is remotely opened/closed by the guard from the control station when an unmanned platform moves into or out of an enclosed area.

Fig. 4. MDARS Approaching Legacy PSE Swing-Arm Gate

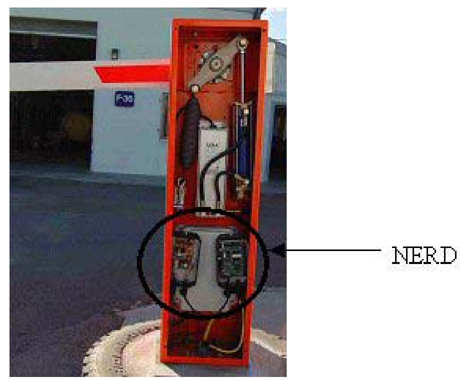

Fig. 5. Network-Enabled Resource Device Controlling PSE

For example, when an MDARS patrol unit stops at a predefined location in front of a closed swing-arm gate, the patrol unit requests clearance from the guard at the control station to open the gate. The guard uses the MRHA to remotely operate the gate using the NERD installed in the gate enclosure (Fig. 5).

Fig. 6. MRHA Operator Station Controlling MDARS and Legacy PSE Swing-Arm Gate

During normal operations, the MRHA autonomously opens the gate, sends the MDARS patrol unit past the gate, and then closes the gate, simultaneously logging all activity. The guard may also monitor the progress using video and status information displayed on the MDARS control station (Fig. 6) and can manually override any action. Any legacy physical security equipment controlled using electro-magnetic devices to open or close, turn on or off, etc., can be interfaced to the MRHA in a similar manner.

c. Force-on-Force Scenario

A demonstration scenario has been developed to test and refine the key technologies for Integrated Force Protection (Fig. 7). The scenario involves two opposing forces, blue and red, each consisting of manned and unmanned assets.

Fig. 7. Integrated Force Protection

The blue force is defending the headquarters with a human guard force stationed in the ROCC. The blue assets include security forces patrolling in guard trucks, MDARS patrol units, fixed and man-deployable sensors, remotely operated weapons, and legacy physical security equipment such as barrier gates. Guard trucks use a NERD with GPS, cameras, and wireless communications to provide location and video to the ROCC. For multi-dimensional operations, UAVs and Unmanned Surface Vehicles (USV), each with cameras and other sensors, can be deployed. The ROCC provides situational awareness including video and status from all friendly resources.

The red forces, or attacking team, are infantrymen using backpackable robots such as URBOTs, Foster-Miller Talons, and iRobot PackBots. The red force is performing a scouting mission on the blue headquarters. The infantrymen teleoperate the robots using suitcase-sized Operator Control Units (OCU) or handheld OCUs with batteries and radios stowed in wearable backpacks. For demonstration purpose, the video feed from the red force is also displayed in the ROCC.

The scenario begins with the red force infiltrating the perimeter defenses of the blue headquarters. The red force monitors the MDARS patrol unit being dispatched from the headquarters to perform random patrols around the base. When the MDARS leaves, the red backpackable robot leaves its hiding place and begins its assault.

An unattended sensor stationed outside of the building detects the movement of the red force. A Distributed Interactive Video Arrays (DIVA) sensor network tracks the intruder and notifies the guard at the operator station in the ROCC. The MDARS vehicle may be autonomously deployed to an overwatch station to provide a better vantage point to monitor the red force or may be directed by the operator to intercept the intruders. A second MDARS patrol unit, parked in a garage for second shift operations, is prepared for duty. It is remotely turned on and the garage door is automatically opened before the MDARS unit is dispatched.

The red forces, unaware that they have been detected, continue their assault into the main building complex. Once the force enters, the guard takes control of the audio challenge and non-lethal weapon. After the red force ignores the initial verbal challenge, the operator aims and fires the weapon at the invaders. The non-lethal weapon can fire pepper-spray balls to disable a human intruder or florescence paint to mark human/unmanned forces. The red forces retreat and escape the building.

MDARS allows the ROCC operator to direct mobile sensors to the area of interest in order to return more relevant data about the intruder. MDARS displays the video of the primary intruder and locations with track histories of all intruders. UAVs and USVs are deployed in their respective areas to look for additional threats or help give additional situational awareness to the current area of intrusion. Barrier gates that control vehicular traffic to the area are automatically opened by the MRHA and MDARS enters into the headquarters area.

A manned guard truck is alerted of the threat and returns to headquarters. The guard at the ROCC console can track the position and out-the-window video of the truck. Red forces go off road and are tracked by a remote perimeter radar unit stationed near the fence line. A marsupial URBOT is deployed from the MDARS patrol unit to monitor the actions of the red force. Blue manned and unmanned forces are coordinated by the ROCC to surround the hostile forces and capture the red team.

4. FUTURE OPERATIONS

a. MDARS Spiral Development

SSC San Diego is leading technology advancements for MDARS spiral development including communications, payloads, and user interfaces.

MDARS payload systems are designed in a modular fashion for "plug-n-fight" capability. The payloads can be quickly configured to operate from either an unmanned vehicle, a manned military vehicle such as a HMMWV, or standalone as unattended munitions or automated mission modules. In FY-03, both payloads were demonstrated standalone and mounted on a MDARS patrol unit. In FY-04, plans are to demonstrate 2nd generations of the weapons pod and UAV launcher mounted on an USV and a manned vehicle. These efforts expand force protection and force-multiplication potential for unmanned vehicles.

As described above, the MRHA interfaces to unattended ground sensors. The MRHA also monitors fixed volumetric motion sensors that are part of installed (legacy) security systems. In FY-04, the MRHA will operate on the same console as the Integrated Commercial Intrusion Detection System (ICIDS-III) to share alarm data from all sensors. The goal is a seamless user interface to display a common operational picture from all the mobile sensors on the MDARS patrol units and the fixed sensors in the ICIDS-III infrastructure.

SSC San Diego is a contributor to the JAUS development of message sets for internal and external communications for unmanned vehicles. In FY-03, the JAUS Operator Control Unit (OCU) and Payload Committee planned a sequence of experiments to demonstrate and expand the level of interoperability between OCUs and unmanned vehicles. SSC San Diego hosted and participated in the first JAUS OCU and Payloads Committee experiment where nine organizations implemented a JAUS message set for teleoperation on for six different unmanned systems – each consisting of an OCU and an unmanned ground vehicle (Fig. 8). Each OCU was then able to monitor the status of every UGV and each OCU could take individual control and teleoperate any of the unmanned vehicles. In FY-04, SSC San Diego and the JAUS Working Group will expand the experimentation domain to assess JAUS message sets required for payloads and missions.

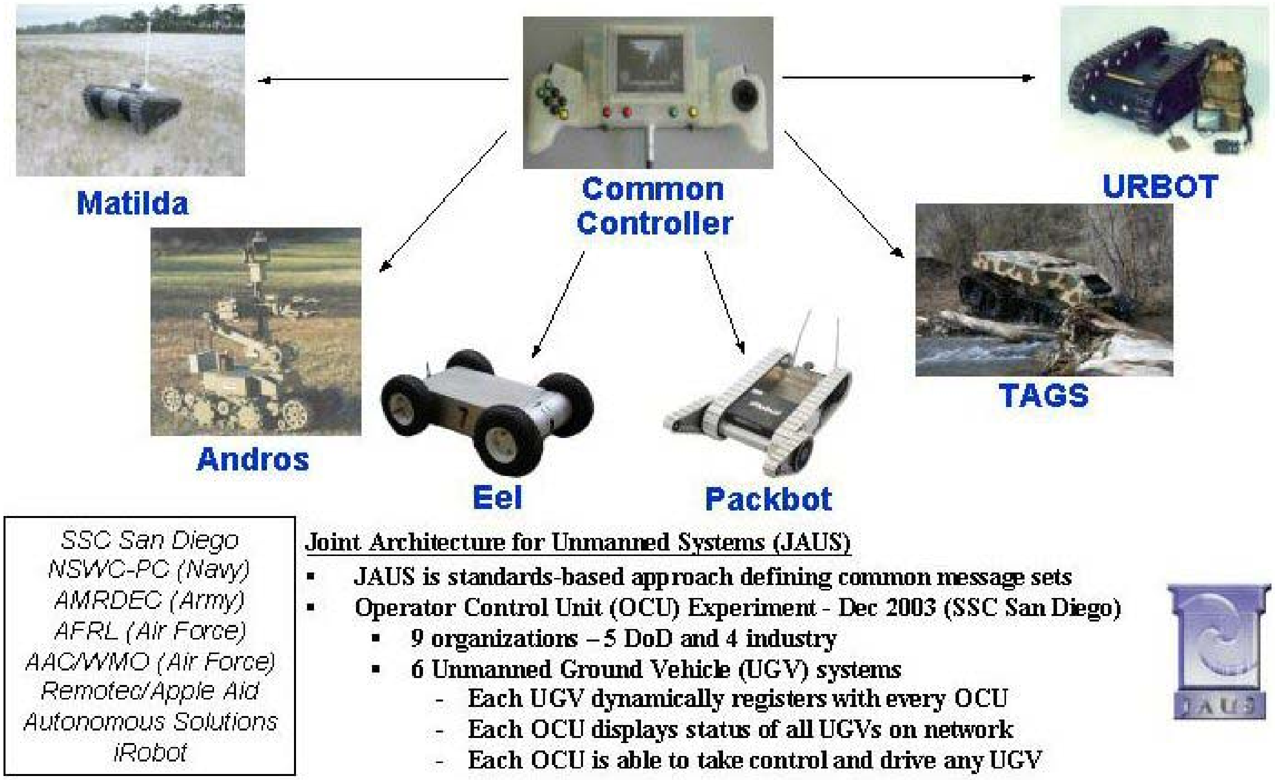

Fig. 8. JAUS OCU and Payload Committee Experiment

SSC San Diego is also collaborating with the Air Force Research Laboratory (AFRL) Robotics Group, Tyndall AFB, Panama City, FL, to employ JAUS for the REDCAR initiative. SSC San Diego is extending the communications, user interfaces, and payloads subsystems for MDARS to use JAUS messages for REDCAR demonstrations in FY-04.

b. REDCAR Proof of Concept

The FPB entered into a major partnership with AFRL to develop the REDCAR system and with SSC San Diego to support the initiative. The goals of the current phase are to develop and integrate a family of unmanned ground vehicles, each conducting part of the REDCAR mission, including overlap of capability to allow for redundancy and to facilitate handover to the appropriate system. The REDCAR proof of concept (Fig. 9) deploys three robotic platforms: SCOUT, MDARS, and PackBot.

The AFRL Robotics Group is the designer of the SCOUT unmanned ground vehicle. The SCOUT vehicle has waypoint navigation using obstacle avoidance and anti-roll sensing. After detecting an obstacle, the vehicle steers away from the collision point. The vehicle also determines the rate of turn against forward speed to assess roll potential and automatically slows itself to an acceptable speed to prevent rollover. SCOUT is equipped with a thermal imager, image intensifier and low-light daytime CCD cameras. The third generation image intensifier sees through glass and features a high-resolution black and white image that shows images in ultra fine detail. The camera has a pan and tilt assembly that can be finely controlled by responsive worm drives for azimuth and elevation corrections. The SCOUT is also configured to carry a non-lethal or lethal payload, along with the audio challenge system.

Built into the REDCAR control unit is a touch screen, allowing the operator to switch between sensors. An autoscan facility is available for use when the unmanned ground vehicle is in an over watch position.

The SCOUT is based on a Polaris 4x4 ATV and it is still possible to drive the vehicle in a conventional sense - i.e. the driver sits on the vehicle and engages normal drive mode. This design has advantages in that a Security Forces member can be conducting ordinary patrol duties, yet can dismount if an incident is potentially dangerous and allow the vehicle to move into harm's way and conduct surveillance. This provides Security Forces personnel with the ability to achieve situational awareness yet retain a protective posture until it becomes necessary to intervene.

The MDARS platform performs surveillance for both initial detection during random patrols and from a deployed over watch position to support the SCOUT platform for challenge actions.

The PackBot is a robust and portable robot for urban operations. The machine can be carried by one or more of the other engagement or surveillance platform (as a marsupial) or be driven into a building through a window, climb stairs, or operate in the small places that the larger platforms can not get to. It also carries an array of cameras or sensors, mission dependent. For example, PackBot missions could include searching in tunnels to locate for enemy soldiers that may be hiding or remotely examining discarded equipment that may be potentially booby-trapped. PackBots are currently in use in operations in Afghanistan and Iraq. The PackBot is designed as a marsupial type vehicle to enter confined locations inaccessible to the larger platforms.

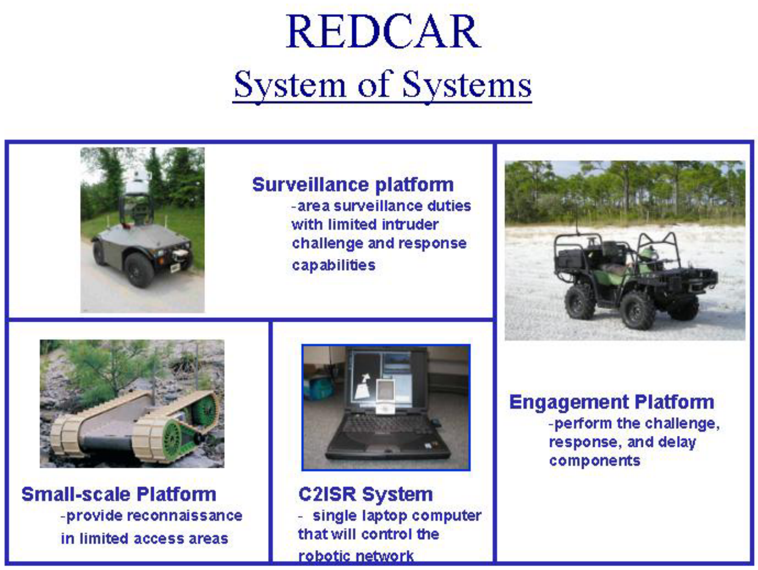

Fig. 9. REDCAR System of Systems (graphic courtesy of the AFRL Robotics Group)

A critical element of an unmanned security response involves the acts of both challenge and causing delay. To keep the system within the legal realms of force protection, research was done to mirror the Air Force's Use of Force Continuum model. This dictates that as the risk or situation elevates so does the level of response/actions by the security forces. The first step in the REDCAR phase is that the main surveillance platform will be parked with warning/operation lights and reflectors. This meets the first safety aspect in that others can see the robotic platform moving both day and night. It is a visible deterrent at the same time. The next step is to add lights or rather spot/beam lights to pinpoint an area, obstacle or intruder. The specific light produces a light intensity of 6 million candlepower. This meets the elevated threat response by providing an actual physical engagement between a known or perceived authority with an intruder. Should the situation elevate from there a recognizable voice "challenge" is issued. (NOTE: This challenge can come from the surveillance platform, which is highly recognizable, or the engagement platform, which is not readily recognizable. The decision to employ either platform is determined by the owner/user agency, as they desire following their own set of rules of engagement. Specific tactics, techniques and procedures for integrating robots with the current fielded forces are being investigated.

The REDCAR challenge phase involved many technical challenges. First was the need to give an audible challenge that could be heard and understood over the noise of the REDCAR vehicle engine. Second was the need to project the challenge at a distance so that the adversary could not physically attack the vehicle.

The challenge requirement must be met in both English and in the local language and dialect. Suitable technology was needed to fill this gap, enabling both the ability to offer increasing levels of warning and in the local language of the theater of operation. Research led to DARPA, and Project Babylon. The goal of Babylon was to produce a hand-held device able to rapidly translate English phrases into a foreign language, and eventually translate phrases from a foreign language into English. The REDCAR initiative chose the Phraselator as its translator system. The Phraselator Translation System is a voice-activated handheld system that translates predetermined phrases into the desired foreign language, allowing users to accurately convey critical information in real-time - without a human translator.

The Phraselator offer typical phrases for topic areas such as force protection and initial medical encounters. At this stage of development, the Phraselator can translate from English into one of 42 languages/dialects. Once the vehicle is in position to make the challenge, the operator will assesses the situation and choose the right phrase. Phraselator will translate the phrase into the chosen dialect. A planned improvement is for the system to automatically translate the response from the intruder into English, allowing for two-way conversation.

Fig. 10. REDCAR SCOUT (graphic courtesy of the AFRL Robotics Group)

If the intruder takes further evasive action against the robotic platforms and further progress towards the protected resource, the REDCAR system would employ the currently approved non-lethal weapon (CS Gas) as determined by the human operator. If the situation were to continue to escalate, so would the level of force necessary to deal with the threat. The human operator makes the final decision to employ the lethal (deadly force) weaponry. (At no time does the robotic system make the autonomous determination to employ or not employ force). Currently the SCOUT platform (Fig. 10) carries a standardized mounted M-16 rifle and ammunition, negating the need to create a specialized weapon or specialized ammunition for the REDCAR concept. Locally issued weapons and ammunition is fitted into the engagement platform. The ammunition system can use a normal issue single 30 round magazine or a single 100 round ammunition magazine, both of which are in the Air Force inventory.

In parallel, the Air Force Electronic System Center (ESC) is developing the IBD Security System (IBD SS). This system of systems is intended to integrate all of the sensor and surveillance systems, improving situational awareness by providing a common operating picture to the defense or wing commander. The REDCAR system will also be integrated into the IBD SS, taking information from an external sensor leading to a robotic response, or in turn providing detection to allow other systems to respond.

5. CONCLUSIONS

The USAF Remote Detection Challenge and Response (REDCAR) initiative take advantage of a System of Systems of unmanned vehicles for Integrated Base Defense. REDCAR integrates the US Army Mobile Detection Assessment Response System (MDARS) with the Air Force Research Laboratory Robotics Group SCOUT.

MDARS is Force Protection system that deploys autonomous patrol units for surveillance and security. The Multiple Resource Host Architecture (MRHA) is the MDARS Control Station software to simultaneously control heterogeneous unmanned systems. The Robotics Operation Command Center unites command and control (C2) with unmanned systems to provide Integrated Force Protection.

REFERENCES

1. Carroll, D., Gilbreath, G.A., Grant, K., and L. Day, “Command and Control for Mixed Manned and Unmanned Security Forces”, Unmanned Systems in International Security 2003, London, UK, September 11, 2003.
2. USAF Security Forces, “Integrated Base Defense (IBD) 2020 Technology Architecture (Draft)”, July 2003.